DT01 Rec'd PCT/PTC 20 DEC 2004

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) Method of generating electronic keys d for a public-key cryptography method using an electronic device, ~~mainly characterized in that it comprises~~ comprising the following two separate calculation steps:

Step A

1) calculating pairs of prime numbers (p,q) or values representative of pairs of prime numbers, this calculation being independent of knowledge of [[the]] a pair of values (e,l) in which e is the public exponent and l is the length of the key of the cryptography method, ~~l also being the length of the modulus N of said method,~~

2) storing the pairs or values thus obtained; and

Step B

calculating a key d from the results of step A and knowledge of the pair of values (e,l).

2. (Currently Amended) Method of generating electronic keys according to Claim 1, ~~characterized in that~~ wherein step A-1) ~~consists in~~ comprises calculating pairs of prime numbers (p, q) without knowledge of the public exponent e or of the length l of the key, using a parameter Π which is the product of small prime numbers, so that each pair

(p, q) has a maximum probability of being able to correspond to a future pair (e,l) and can make it possible to calculate a key d.

3. (Currently Amended) Method of generating electronic keys according to Claim 2, ~~characterized in that~~ wherein the calculation of step A-1) also takes account of the fact that e has a high probability of forming part of the set {3, 17, ..., [[2^{16+1}}]] $2^{16}+1$}, and ~~for this use is made in the calculation of~~ using a seed σ in the calculation which makes it possible to calculate ~~not pairs (p,q) but~~ a representative value ~~referred to as the~~ constituting an image of the pairs (p, q).

4. (Currently Amended) Method of generating electronic keys according to ~~Claims 1 and 3, characterized in that~~ claim 3, wherein the storage step A-2) ~~consists in~~ comprises storing the image of the pairs.

5. (Currently Amended) Method of generating electronic keys according to Claim ~~1, characterized in that~~ 2, wherein step A-1) ~~consists in~~ comprises calculating pairs of prime numbers (p, q) for different probable pairs of values (e,l).

6. (Currently Amended) Method of generating electronic keys according to ~~Claims 2 and 5, characterized in that~~ claim 5, wherein the parameter Π contains the ~~usual~~ values ~~of the public exponent e, for example~~ 3, 17.

7. (Currently Amended) Method of generating electronic keys according to Claim 1, ~~characterized in that~~ wherein step A-1) comprises an operation of compressing the calculated pairs (p,q) and step A-2) ~~then consists in~~ comprises storing the compressed values thus obtained.

8. (Currently Amended) Method of generating electronic keys according to Claim ~~1, characterized in that~~ 3, wherein step A-1) comprises the generation of a prime number q for which a lower limit B_0 is set for the length ℓ_0 of this prime number that is to be generated, such that $\ell_0 \geq B_0$, ~~for example $B_0 = 256$ bits,~~ and ~~in that it comprises~~ further comprising the following sub-steps:

1) calculating parameters v and w from the following relations and storing them:

$$v = \sqrt{2^{2\ell_0 - 1}} / \Pi$$

$$w = 2^{\ell_0} / \Pi$$

in which Π is stored and corresponds to the product of the f smallest prime numbers, f being selected such that $\Pi \leq 2^{B_0}$,

2) selecting a number j within the range of integers $\{v, \ldots, w-1\}$ and calculating $\ell = j\,\Pi$;

3) selecting and storing a prime number k of short length compared to the length of an RSA key within the range of integers $\{0, \ldots, \Pi-1\}$, (k, Π) being co-prime;

4) calculating $q = k + \ell$,

5) verifying that q is a prime number, if q is not a prime number then:

a) taking a new value for k using the following relation:

$k = a\ k \pmod{\Pi}$; a belonging to the multiplicative group Z^*_{Π} of integers modulo Π;

b) repeating the method from step 4).

9. (Currently Amended) Method of generating electronic keys according to ~~Claims 3 and 8, characterized in that~~ claim 8, wherein the numbers j and k can be generated from the seed σ stored in memory.

10. (Currently Amended) Method of generating electronic keys according to Claim 8, ~~characterized in that~~ wherein the prime number p is generated by repeating all the above sub-steps while replacing q with p and replacing ℓ_0 with ℓ-ℓ_0.

11. (Currently Amended) Method of generating electronic keys according to ~~any one of the preceding claims, characterized in that~~ claim 1, wherein:

step B comprises, for a pair (p,q) obtained in step A:

- verifying the following conditions:

  (i) p-1 and q-1 are prime numbers with a given e and

  (ii) $N=p^*q$ is an integer of given length ℓ,

- if the pair (p,q) does not satisfy these conditions:
- selecting another pair and repeating the verification until a pair is suitable,
- calculating the key d from the pair (p,q) obtained.

12. (Currently Amended) Secure portable object able to generate electronic keys d of an RSA-type cryptography algorithm, ~~characterized in that it comprises at least~~ comprising:

- communication means for receiving at least one pair of values (e,l),

- a memory for storing the results of ~~a step A consisting in:~~ calculating pairs of prime numbers (p,q) or values representative of pairs of prime numbers, this calculation being independent of knowledge of the pair of values (e,l) in which e is [the] a public exponent and l is the length of the key of the cryptography method, ~~l also being the length of the modulus N of this p~~, and

- a program for ~~implementing a step B consisting in:~~ calculating a key d from the stored results ~~of step A~~ and knowledge of a received pair of values (e,l).

13. (Currently Amended) Secure portable object according to Claim 12, ~~characterized in that it also comprises~~ further comprising a program for ~~implementing step A, steps A and B~~ calculating said results stored in memory, the calculation of said results being separate in ~~terms of~~ time from the calculation of the key d.

14. (Currently Amended) Secure portable object according to Claim 13, ~~characterized in that~~ wherein the program for ~~implementing step A~~ calculating said results carries out the following sub-steps:

1) calculating parameters v and w from the following relations and storing them:

$$v = \sqrt{2^{2\ell_0-1}} / \Pi$$

$w = 2^{\ell_0} / \Pi$

in which Π is stored and corresponds to the product of the f smallest prime numbers, f being selected such that $\Pi \leq 2^{B_0}$, and B_0 is a lower limit set for the length ℓ_0 of the prime number that is to be generated, such that $\ell_0 \geq B_0$, ~~for example B_0 = 256 bits~~

2) selecting a number j within the range of integers {v, ..., w-1} and calculating $\ell = j\,\Pi$;

3) selecting and storing a prime number k of short length compared to the length of an RSA key within the range of integers {0, ..., Π-1}, (k, Π) being co-prime;

4) calculating $q = k + \ell$,

5) verifying that q is a prime number, if q is not a prime number then:

a) taking a new value for k using the following relation:

$k = a\,k \pmod{\Pi}$; a belonging to the multiplicative group Z^*_{Π} of integers modulo Π; and

b) repeating the method from step 4).

15. (Currently Amended) Secure portable object according to Claim 12 ~~or 13 or 14, characterized in that it consists of~~, wherein said object is a chip card.

16. (New) Method of generating electronic keys according to Claim 1, wherein step A-1) comprises calculating pairs of prime numbers (p, q) for different probable pairs of values (e,l).

17. (New) Method of generating electronic keys according to Claim 1, wherein step A-1) comprises the generation of a prime number q for which a lower limit B_0 is set for the length ℓ_0 of this prime number that is to be generated, such that $\ell_0 \geq B_0$, and further comprising the following sub-steps:

1) calculating parameters v and w from the following relations and storing them:

$$v = \sqrt{2^{2\ell_0 - 1}} / \Pi$$

$$w = 2^{\ell_0} / \Pi$$

in which Π is stored and corresponds to the product of the f smallest prime numbers, f being selected such that $\Pi \leq 2^{B_0}$,

2) selecting a number j within the range of integers {v, ..., w-1} and calculating $\ell = j\,\Pi$;

3) selecting and storing a prime number k of short length compared to the length of an RSA key within the range of integers {0, ..., Π-1}, (k, Π) being co-prime;

4) calculating $q = k + \ell$,

5) verifying that q is a prime number, if q is not a prime number then:

a) taking a new value for k using the following relation:

$k = a\,k \pmod{\Pi}$; a belonging to the multiplicative group Z^*_{Π} of integers modulo Π;

b) repeating the method from step 4).

18. (New) Method of generating electronic keys according to Claim 17, wherein the prime number p is generated by repeating all the above sub-steps while replacing q with p and replacing ℓ_0 with ℓ-ℓ_0.